IN THE CLAIMS:

Please cancel claims 2 and 9 without prejudice.

Please amend claims 1, 3-5, 7-8, 10-16, and 18-21 as indicated below.

Please add claim 24 as indicated below.

A listing of the status of all claims 1-24 in the present patent application is provided below.

1. (Currently Amended) A method for assembling fragmented network traffic, comprising:

detecting, by a monitoring node, an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

reassembling the two or more fragments according to the configuration information associated with the destination node.

~~detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a~~

~~corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;~~

~~initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and~~

~~a query to determine configuration information associated with how the destination node is configured to reassemble overlapping fragments.~~

2. (Canceled) ~~A method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap.~~

3. (Currently Amended) [[A]] The method as recited in claim [[2]] 1 wherein determining that said two or more fragments have overlapping offsets ~~overlap~~ comprises reading a header value associated with one of the fragments.

4. (Currently Amended) [[A]] The method as recited in claim 3 wherein the header value comprises an offset value.

5. (Currently Amended) [[A]] The method as recited in claim 1 wherein detecting an anomaly comprises determining that said two

or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments.

6. (Canceled)

7. (Currently Amended) [[A]] The method as recited in claim 1 wherein performing a query includes querying the destination node.

8. (Currently Amended) [[A]] The method as recited in claim 1 wherein performing a query includes querying an information base.

9. (Canceled)

10. (Currently Amended) [[A]] The method as recited in claim 1 further including processing the anomaly to determine whether the fragmented network traffic is associated with a threat.

11. (Currently Amended) [[A]] The method as recited in claim 1 further including performing an action on the fragmented network traffic based on whether the fragmented network traffic is

associated with a threat.

12. (Currently Amended) [[A]] The method as recited in claim 1 further including discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat.

13. (Currently Amended) [[A]] The method as recited in claim 1 further including copying one or more fragments comprising the fragmented network traffic to a buffer.

14. (Currently Amended) [[A]] The method as recited in claim 1 further comprising ~~wherein performing further processing comprises~~ sending an alert if an anomaly is detected.

15. (Currently Amended) [[A]] The method as recited in claim 1 ~~wherein performing further processing comprises~~ further comprising determining whether the fragmented network traffic should be blocked.

16. (Currently Amended) [[A]] The method as recited in claim 1 ~~wherein performing further processing comprises~~ further comprising determining whether the fragmented network traffic

should be forwarded to the destination node.

17. (Canceled)

18. (Currently Amended) [[A]] The method as recited in claim 1 ~~wherein performing further processing comprises~~ further comprising determining that two or more fragments contained in said fragmented network traffic have overlapping portions.

19. (Currently Amended) [[A]] The method as recited in claim 1 wherein detecting an anomaly comprises determining that two or more fragments contained in said fragmented network traffic have mismatching overlapping portions.

20. (Currently Amended) A system for assembling fragmented network traffic, comprising:

a memory configured to store at least a portion of the fragmented network traffic; and

a processor configured to:

~~detect in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a~~

~~corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;~~

detect an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

~~initiate in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and~~

perform a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

~~a query to determine configuration information associated with how the destination node is configured to reassemble overlapping fragments.~~

reassemble the two or more fragments according to the configuration information associated with the destination node.

21. (Currently Amended) A computer readable storage medium comprising computer instructions for assembling fragmented network traffic, including instructions for:

~~detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;~~

~~initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and~~

~~a query to determine configuration information associated with how the destination node is configured to reassemble overlapping fragments.~~

detecting, by a monitoring node, an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

reassembling the two or more fragments according to the configuration information associated with the destination node.

22. (Previously Presented) The system of claim 20 wherein performing a query includes querying the destination node.

23. (Previously Presented) The system of claim 20 wherein performing a query includes querying an information base.

24. (New) The method of claim 1, further comprising initiating expanded buffering of fragments contained in said fragmented network traffic in response to detecting the anomaly.